Cryptographic techniques used to provide integrity of digital content under long-term storage

Polish Security Printing Works (PWPW)

Background

Increasing amount of data, both created and stored electronically, entails the necessity to construct various data storage systems. In view of different requested storage periods, we divide systems into:

- short-term – storage period no longer than 3 years,
- medium-term – storage period between 3 and 10 years,
- long-term – storage period longer than 10 years but with the specified end-date,
- unlimited – storage period longer than 10 years with not specified end-date.

The unlimited storage is sometimes called the “eternal” one. In this case we have to pay special attention to the integrity of stored digital content. Because of that, various digital marking techniques are used, and even after long time one is able to verify the integrity of stored data.

Problem description

The main objective is to use advanced mathematical methods, especially cryptographic techniques used in the process of digital marking of content. These techniques should guarantee verification the integrity of long-term-stored digital content.

The proposed methods should take into account :

- different kinds (classes) of stored content, e.g. cultural heritage, court documentation, accounting documentation, etc.;
- database size limitations;
- anticipated frequency of access to stored resources;
- …

Another very important aspect of the problem is to define the limits of advanced mathematical methods, especially those based on cryptographic techniques, and to check the applicability of those methods in the diagnostics of data loses (e.g. due to "corrosion" of media) as well as in potential data recovery.

Special attention should be paid to:

- Systems and schemes of coding, which allow detection and correction of write errors.
- Cryptographic techniques, such as:
    - public-key and asymmetric encryption,
    - secret sharing methods,
    - secure multiparty computations.